Amendment to the Specification

Please amend the specification as follows:

Please replace the paragraph starting at page 2, line 13 with the following:

In **FIGURE 1**, cable system 100 is shown. Content Encryption Block 104, conditional access management system 108 and television Set-Top Box STB 112 are also shown. Within content encryption block 104 (content encryption block 104 and CA management system 108 are generally located at the cable system headend or content distribution broadcast center) are Simulcrypt™ Synchronizer (SCS) Processor 116 and content encryption block 120. Within the content encryption block 120 are code word generator 124 and encrypt engine 128. Output multiplexer (mux) 132 is the final block within content encryption block 104. Details of the communications interfaces within cable system head end will follow. The interfaces described may be hardware interfaces with direct connections as shown or software interfaces for communication over, for example, a bus structure without limitation.

Please replace the paragraph starting at page 2, line 13 with the following:

Within conditional access management system 108 are the content scheduler 136, the event information scheduler (EIS) 140, the subscriber database 144, the ECM generator 148 and the EMM generator 152.

Please replace the paragraph starting at page 3, line 5 with the following:

Communications between the content encryption block 104 and conditional access management system 108 occurs over the encryption device to conditional access system communications link 172. Conditional access system communications link 172 is composed of several other interfaces, namely access criteria interface 176, code word and access criteria interface 180 and signed ECM interface 184.

Please replace the paragraph starting at page 3, line 18 with the following:

Likewise, EMM generator 152 interfaces with subscriber database 144 across subscriber database interface 192 to retrieve information necessary to create EMM messages. ECM

generator 148 and EMM generator 152 communicate across ECM/EMM interface 196 to communicate information that is necessary for ECM generator 148 to create signed ECM messages. EMM packets are transferred to STB 112 across EMM packet interface 1100 and signed ECM messages are transferred from ECM generator 148 to SCS processor 116 across signed ECM interface 184 to complete the current actions of the conditional access management system 108.

Please replace the first paragraph of page 15 with the following:

Turning now to **FIGURE 2**, an illustrative Default Multi-channel Encryption System (DMES) 200 is shown. This figure builds on **FIGURE 1**, with the addition of default configuration memory 204 which is used to store default encryption information for situations of communication failure between content encryption block 104 and conditional access management system 108. One of the possible multiple conditional access systems within the cable system head end is shown as conditional access management system 108. Conditional access management system 108 is responsible for, among other things, assuring encryption of ~~encrypting~~ the content of each program that is broadcast from the cable system head end using content encryption block 104. Encryption keys and other related, time-varying information is generated in content encryption block 104 as discussed above and in the published DVB specification. Content encryption block 104 behaves as a conditional access encryption ~~management~~ system.

Please replace the paragraph at page 15 line 13 with the following:

As mentioned above, this encryption information is changed periodically, occasionally, or according to any defined schedule so that content encryption block 104 and conditional access management system 108 attempt to remain in communication, subject to the difficulties discussed above, via conditional access system communications link 172.

Please replace the paragraph at page 15, line 13 with the following:

In order to resolve the difficulties associated with a loss or absence of communication

between conditional access management system 108 and the remainder of the cable system head end, default configuration memory 204 is provided. Default configuration memory 204 can be any non-volatile storage mechanism, such as Flash memory, ROM memory, battery backed up memory, disc storage, or any other suitable computer readable storage medium, so that its contents are persistent through power cycles of the system. Default configuration memory 204 is connected to SCS processor 116 via CA memory interface 208.

Please replace the paragraph starting at page 16, line 3 with the following:

Once initialized, the presence of the default configuration memory 204 allows content encryption block 104 to read default encryption keys and other related information associated with the cable channels in the event of a communication loss between itself and conditional access management system 108. Accordingly, under any of the situations discussed above, content encryption block 104 will always have a capability for encryption using a default encryption key for each cable channel once initialized and provisioned. This prevents broadcast of objectionable and/or premium content (or any other designated content) in the clear to prevent unauthorized recipients from viewing the content. It should be noted that even if the system contains no receiver devices (e.g., STBs) that are appropriately outfitted (as will be described later) to receive content that is encrypted under the default encryption keys, it is often preferred for paid viewers to have their programming disrupted than to have objectionable or otherwise normally protected content transmitted without benefit of encryption.

Please replace the paragraph starting at page 16, line 24 with the following:

Turning now to **FIGURE 3**, an illustrative default encryption information retrieval method 300 is shown. At 304, the method begins. At 308, the process determines whether the communication channel between the conditional access management system 108 and the content encryption block 104 is active and functioning properly or whether there has been a communication failure. Note that, in certain embodiments, the attempted communication occurs every few seconds (or faster), so detection of communication loss or restoration may have a very low latency. If a communication failure has not occurred at 308, a transition is made to 312 to

carry out communications to transmit encryption keys and related information from content encryption block 104 of cable system head end to conditional access management system 108 for all channels in the system. Otherwise, if a communication failure is determined to have occurred at 308, a transition is made to 316 where encryption keys and related information is read from the default configuration memory 204 until communication is restored. The communication channel is again checked at 308 where the process repeats during the current power cycle of the equipment.

Please replace the paragraph starting at page 17, line 11 with the following:

Turning now to **FIGURE 4**, an illustrative Default Multi-channel Decryption System (DMDS) 400 is shown. To further extend the capability and to accommodate legally authorized STB's to view content scrambled with a fixed key as described above, an alternative embodiment provides for assignment of a default key or keys to the STB (or other receiver device). In this manner, those legally authorized STBs can be signaled and can temporarily use the default fixed key(s) to descramble content until such time as the live keys can again be injected into the stream. One possibility for the signaling is a specially formatted ECM, originating from the encryption device (since the conditional access management system 108 to the content encryption block 104 connectivity has been lost) and signaling the STB to resort to a fixed-key mode.

Please replace the paragraph starting at page 18, line 14 with the following:

Turning now to **FIGURE 5**, an illustrative default encryption information retrieval method 500 is shown. This diagram is very similar to **FIGURE 3** above with the addition of signaling blocks and is carried out at the cable system head end at content encryption block 104. At 504, the method begins. At 508, the process determines whether the communication channel between the conditional access management system 108 and the content encryption block 104 is active and functioning properly or whether there has been a communication failure. If a communication failure has not occurred at 508, a transition is made to 512 to carry out communications to transmit encryption keys and related information from content encryption

block 104 to conditional access management system 108 for all channels in the system. Then at 516, a global signaling to the STBs in the system is done to instruct the STBs to extract encryption keys from the data stream.

Please replace the paragraph starting at page 19, line 15 with the following:

In the case of a communication failure between the content encryption block 104 and the conditional access management system 108, no valid active key(s) would be received. In this case, fixed default key(s) and/or instructions to switch to using the default fixed key(s) are provided. Likewise, new fixed default key(s) can be transmitted based upon the decisions of the cable system provider even without a communication failure in the content encryption block 104. At 612, a determination is made as to whether there are new fixed default key(s). If there are, they can be stored to memory at 616. If there are no new default fixed key(s) to store at 612 or the storage is complete at 616 a transition is made to 620.